EideBailly®

CPAs & BUSINESS ADVISORS

CLOUD RISKS AND MYTHS FOR 2020

October 2019

1

MEET YOUR PRESENTER

Calvin Weeks
Digital Forensics | Forensic Response

- 30+ years in Digital Forensics & Cyber Security
- Certifications
  - Certified Information Security Manager (CISM)
  - Certified Information System Security Professional (CISSP)
  - Certified in Risk and Information Systems Control (CRISC)
  - Certified E-Discovery Specialists (CEDS)
  - EnCase Computer Forensics Examiner (EnCE)
  - Certified Steganography Examiner (CSE).
- Testimony Experience
  - Local, State, and Federal courts

2

CLOUD RISK AND MYTHS FOR 2020

If you do not have technology or applications in the cloud then you will or you will be left behind. Moving to the cloud is not without risk and if you do not understand how to address those risks then the cloud move will be a disaster for you. You need to understand some basic differences in operating on your premises versus in the cloud, new risks, and security concerns. This presentation will help you be aware of the risks, security, and myths of cloud based computing trends for 2020.

3

TOPICS

- What do we mean by "cloud"?
- Common Myths
- Cloud Risks
- Cloud Security Concepts

4

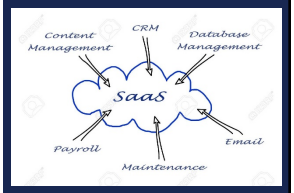
WHAT DO WE MEAN BY "CLOUD"?

5

SOFTWARE AS A SERVICE (SAAS)

Examples include:

- Office 365
- Adobe
- Google Apps
- Salesforce
- Dropbox
- MailChimp
- ZenDesk
- DocuSign
- Skype
- Slack
- Hubspot
- proprietary applications



6

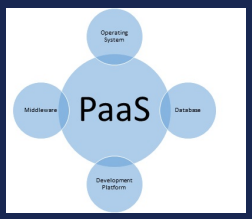
WHAT DO WE MEAN BY CLOUD

7

PLATFORM AS A SERVICE (PAAS)

Examples include:

- Operating systems
- Database
- Web server
- AWS Elastic Beanstalk
- Heroku
- Force.com
- OpenShift
- Apache Stratos
- Magento Commerce Cloud



8

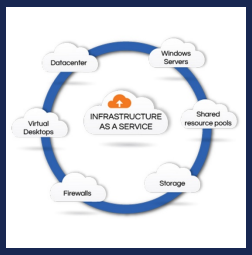
WHAT DO WE MEAN BY CLOUD

9

INFRASTRUCTURE AS A SERVICE (IAAS)

Examples include:

- AWS
- Azure
- Google Cloud
- Rackspace
- Digital Ocean
- Private



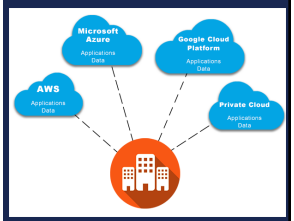
10

WHAT DO WE MEAN BY CLOUD

11

MULTICLOUD & HYBRID

- Multiple different public cloud services, often from multiple different providers
- Hybrid always includes private and public



12

COMMON MYTHS

13

CLOUD MYTH

Going to the cloud is quick and easy.

Generally speaking it can be, but migrating to the cloud requires planning, time, and expertise.

14

CLOUD MYTH

Data in the cloud is public.

Not true. You can have public access, private access, and restricted access.

15

CLOUD MYTH

More breaches occur in the cloud.

Any technology that is not secured and maintained properly will have more breaches.

16

CLOUD MYTH

The cloud is more secure or less secure.

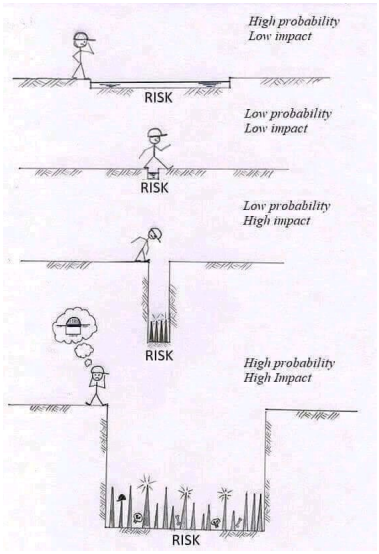
Both can be equally possible. Generally companies underestimate the requirements to move to the cloud thus making the cloud less secure.

17

CLOUD RISKS

18

UNDERSTANDING BASIC RISK



19

CLOUD RISK

Customer and Business contractual breaches.

Contracts among business parties often restrict how data is used and who is authorized to access it. When employees move restricted data into or out of the cloud without authorization, the business contracts may be violated and legal action could ensue. Consider the example of a cloud service that maintains the right to share all data uploaded to the service with third parties in its terms and conditions, thereby breaching a confidentiality agreement the company made with a business partner.

20

It is not a questions of if, but when you will be compromised.

A common understanding with security experts is now:

You will be compromised and you may be compromised already and not know it.

21

CLOUD RISK

Management APIs can be Compromised.

Unlike management application programming interface APIs for on-premises computing, cloud based APIs are accessible via the Internet exposing them more broadly to potential exploitation.

Equivalent to access control over everything.

Threat actors look for vulnerabilities in management APIs. If discovered, these vulnerabilities can be turned into successful attacks, and organization cloud assets can be compromised. From there, attackers can use organization assets to perpetrate further attacks against other cloud customers.

22

EASY TARGETS

49% of victims who were successfully attacked are attacked again with in one year.

It would take a sophisticated hacker only 6 minutes to break into a Wi-Fi network.

23

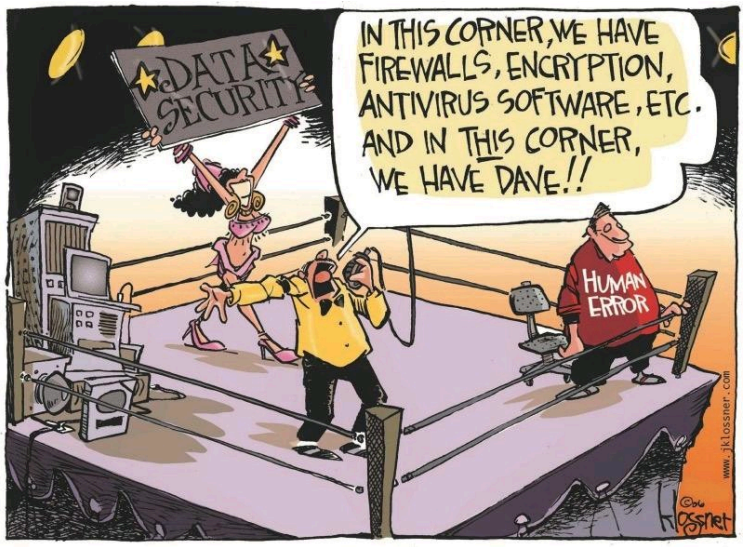
CLOUD RISK

Cannot confirm data deletion.

Data owners has reduced visibility into where their data is physically stored making is difficult to verify secure deletion of their data.

24

HUMAN ERROR



25

CLOUD RISK

Insider unauthorized use.

Insiders, such as staff and administrators for both organizations and cloud service providers (CSP)s, who abuse their authorized access to the organization's or CSP's networks, systems, and data are uniquely positioned to cause damage or exfiltrate information.

The impact is most likely worse when using IaaS due to an insider's ability to provision resources or perform nefarious activities that require forensics for detection. These forensic capabilities may not be available with cloud resources.

26

MEANS OF COMPROMISE

49% of malware is installed via malicious email attachments.

Over 80% of all attacks involve some form of social engineering attack method. They do this by tricking and convincing you to allow them a means to compromise your system or identity.

27

CLOUD RISK

Loss of intellectual property

Organizations are storing more sensitive and protected data in the cloud. During a breach, cyber criminals can gain access to this sensitive data. Absent a breach, certain services can even pose a risk if their terms and conditions claim ownership of the data uploaded to them.

28

TO MAKE MATTERS WORSE

On average it takes 101 days to detect a malware infection.

On average it takes 12 months to detect a hacker has access to your network.

On average it takes more than 3 years to become aware that your identity has been stolen.

29

CLOUD SECURITY CONCEPTS

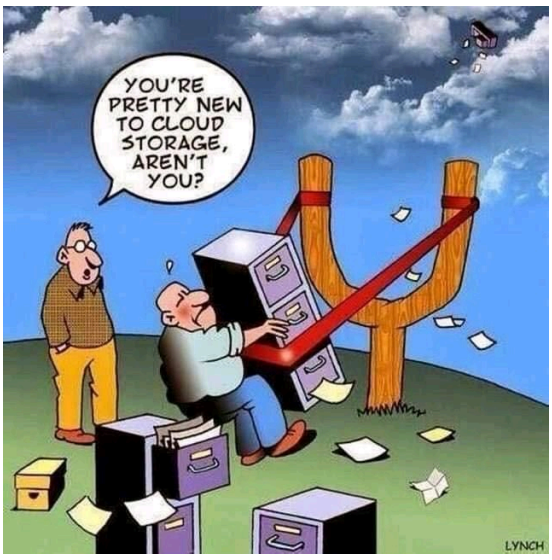
30

BASIC CYBER SECURITY

Simplify Cyber Security with a Balanced Approach:

- Prevent – Use all resources and attempt to prevent all breaches.
- Inventory & Vulnerabilities – Know what technology you have and remediate/mitigate all vulnerabilities.
- Detect – Monitor to detect all attacks.
- Data Flow and Logging – Know what your network/system/application configuration is and ensure you have adequate centralized logging.
- Respond – Respond to all activities that could adversely impact your organization. Making the informed decision to do nothing is acceptable.

31



32

CLOUD SERVICE PROVIDERS SECURITY SOLUTIONS

AWS

- Prevent
  - AWS Identity Access Management & AD Integration
  - VPC Design & Security Grouping
- Detect
  - Cloudwatch Configuration
  - Cloudwatch & Cloudtrail Integration
- Response
  - Automated Response LAMDA

AZURE

- Prevent
  - Secure Access Management
  - Security Grouping and Design
- Detect
  - Microsoft Security Center
  - Azure Advanced Threat Protection
- Response
  - Defender Advanced Threat Protection

33

If you think good architecture is expensive, try bad architecture.

34

STATS

- 33% of IT professionals say cloud security is their biggest skill shortage
- 18.4% say the average enterprise experiences 23.2 cloud-related threats per month
- 18.1% of files uploaded to cloud-based file-sharing and collaboration services contain sensitive data

35

MORE STATS

72% of organizations are committed to confidential or sensitive information in the cloud

50% of organizations have defined roles & accountability for safeguarding sensitive information stored in the cloud

49% of organizations are encrypting sensitive data in the cloud

36

MORE STATS

53% of businesses are controlling the encryption keys when data is encrypted in the cloud

78% of the same businesses are saying it's important to retain ownership of the encryption keys

32% don't employ a security-first approach to storing data in the cloud

37

MORE STATS

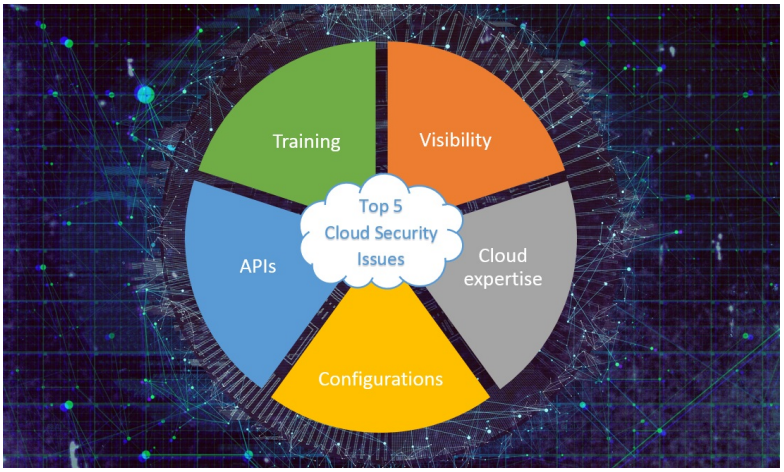
44% of organizations are careful about sharing sensitive information with third parties

60% of organizations are storing customer information, 48% are storing emails, and 46% are storing consumer data

41% of IT and data processing requirements are met by using cloud resources today

38

CLOUD SECURITY ISSUES



39

MY TOP ISSUES TO ADDRESS

- Make security a priority for everything or you will never be able to secure the data in the cloud
- Most cloud services are provided by a third party. READ the agreements to understand that they are not responsible for your data, but what security do they provide you to be able to secure your data. You are responsible to fill the gaps.
- Demand a SOC Type 2/3 from each of your vendors and READ it. This will always have the details of their security and will always include exceptions to there security. Know this because it is your responsibility.
- Use trained and qualified staff to manage your IT and especially the cloud technology
- Awareness training for everyone, IT, and Management.
- Security training for everyone, IT, and Management.
- Follow a framework and standard. The best example for free is National Institute of Standards and Technology (NIST). They set the standards followed by everyone.

40

QUESTIONS?

41

THANK YOU

Calvin Weeks
Forensic Response Manager
cweeks@eidebailly.com
405-594-2051

EideBailly®
CPAs & BUSINESS ADVISORS

42